# INSTRUÇÃO DE TRABALHO Nº 1.215

## TÍTULO: PLANO DE AUDITORIA – SISTEMA DE INFORMAÇÃO - LGPD

### 1. OBJETIVO E CAMPO DE APLICAÇÃO

Esta Instrução de Trabalho tem como objetivo descrever o plano de auditorias relacionadas aos controles do sistema de informação, alinhando-se estritamente com as disposições estabelecidas pela Lei Geral de Proteção de Dados – LGPD (Lei n° 13.709/2018)

### 2. RESPONSABILIDADE

A responsabilidade pela execução de todas as ações descritas nesta Instrução de Trabalho para a realização de auditorias no sistema de informação, assim como a definição de sua frequência, é da área de Tecnologia da Informação.

### 3. APLICABILIDADE

As auditorias conduzidas são aplicáveis para:

- Identificar vulnerabilidades de segurança;
- Garantir conformidade com políticas de segurança e regulamentações;
- Avaliar a eficiência operacional e a integridade dos sistemas;
- Verificar atualizações de software e patches;
- Garantir a conformidade e a eficácia de gestão de senhas.

### 4. PROCEDIMENTO

### 4.1. AUDITORIA – GESTÃO DE SENHAS

#### 4.1.1 Revisão das Políticas e Procedimentos de Senhas:

Verificar se as políticas de senha estão atualizadas e alinhadas com as melhores práticas de segurança.

Assegurar que as políticas incluam requisitos mínimos de complexidade de senha, atualização periódica, restrições de reutilização e outras diretrizes relevantes.

#### 4.1.2 Avaliação da Implementação das Políticas

Verificar se as políticas de senha são aplicadas em todos os sistemas e plataformas relevantes.

Analisar se as políticas estão sendo seguidas por meio de revisão de registros de alterações de senha e logs de acesso.

#### 4.1.3 Análise da Segurança das Senhas

Verificar se as senhas seguem boas práticas de segurança (complexidade, comprimento, falta de padrões previsíveis).

Avaliar a força das senhas armazenadas, se estão adequadamente protegidas e criptografadas.

#### 4.1.4 Revisão de Acesso e Controle

Analisar os níveis de acesso concedidos a diferentes usuários.

Garantir que a autenticação de múltiplos fatores seja implementada quando apropriado.

#### 4.1.5 Revisão de Incidentes Recentes

Investigar incidentes de segurança recentes relacionados a senhas para identificar áreas de melhoria.

### 4.2. AUDITORIA – GESTÃO DE ACESSOS

#### 4.2.1 Revisão de Controles de Acesso

Verificar a adequação dos controles de acesso aos sistemas e dados sensíveis.

Revisar permissões de usuário e níveis de acesso para garantir que estejam alinhados com as funções e responsabilidades.

#### 4.2.2 Análise de Logs e Registros de Auditoria

Revisar registros de acesso, logs de eventos e atividades do sistema para identificar padrões ou atividades suspeitas.

Verificar se existem lacunas na geração ou retenção de logs.

#### 4.2.3 Avaliação de Políticas de Segurança e Auditoria

Verificar se as políticas e procedimentos de segurança de TI estão de acordo com as melhores práticas e regulamentações relevantes.

Assegurar que auditorias internas e externas estejam sendo realizadas regularmente.

#### 4.2.4 Verificação de Segurança Física e Lógica

Avaliar a segurança física dos dispositivos e servidores que armazenam dados sensíveis.

Garantir que as medidas de segurança lógica, como firewalls, antivírus e criptografia, estejam implementadas e atualizadas.

#### 4.2.5 Revisão de Incidentes de Segurança

Analisar incidentes anteriores para identificar pontos fracos ou vulnerabilidades que possam ter permitido acessos indevidos ou adulterações.

### 4.3. AUDITORIA – SERVIDORES, LAPTOPS, ESTAÇÕES DE TRABALHO, ETC

#### 4.3.1 Verificação de Segurança

Avaliação de vulnerabilidades.

Verificação de configurações de antivírus, e regras GPO.

Análise de registros de segurança (logs).

#### 4.3.2 Conformidade e Atualizações

Verificar conformidade com políticas de segurança e regulamentos.

Revisar atualizações de software e patches.

Avaliar a eficácia das medidas de segurança implementadas.

#### 4.3.3 Inventário e Gerenciamento

Criar ou atualizar inventário de hardware e software.

Verificar a conformidade com políticas de licenciamento.

Avaliar o gerenciamento de ativos e seu ciclo de vida.

## 4.4. AUDITORIA – ADULTERAÇÕES E ACESSOS INDEVIDOS

### 4.4.1 Escopo da Auditoria

Identificar os sistemas críticos e sensíveis que necessitam de verificação.

Incluir servidores, laptops e computadores com dados sensíveis ou de alta importância.

### 4.4.2 Avaliação de Integridade e Autenticidade

Verificar a integridade dos arquivos críticos nos sistemas.

Examinar logs de alterações de arquivos e diretórios para identificar mudanças não autorizadas.

### 4.4.3 Controle de Acessos

Revisar os logs de acesso para identificar acessos não autorizados.

Verificar permissões de usuário e grupos em arquivos e diretórios sensíveis.

Analisar logs de autenticação para identificar tentativas de acesso indevidas.

### 4.4.4 Monitoramento de Segurança

Analisar registros de segurança (logs) para detectar padrões incomuns ou suspeitos.

Utilizar ferramentas de detecção de intrusão para identificar atividades anômalas.

### 4.4.5 Análise de Vulnerabilidades

Realizar varreduras de vulnerabilidades nos sistemas para identificar pontos fracos.

Avaliar os sistemas em relação a patches e atualizações de segurança ausentes.

### 4.4.6 Revisão de Configurações de Segurança

Verificar configurações de firewall, antivírus, e outras ferramentas de segurança.

Avaliar políticas de senha e de acesso para garantir que sejam adequadas e aplicadas corretamente.

## 4.5. AUDITORIA – INTRUSÃO DE REDE

### 4.5.1 Escopo da Auditoria:

Identificar todos os firewalls e soluções antivírus em uso na infraestrutura.

Incluir tanto hardware quanto software relacionado à proteção de perímetro.

### 4.5.2 Políticas e Configurações:

Revisar e documentar as políticas de firewall em vigor, incluindo regras de filtragem de tráfego, políticas de acesso, etc.

Verificar se as configurações do firewall estão alinhadas com as melhores práticas de segurança.

### 4.5.3 Regras de Firewall:

Analisar as regras de firewall existentes para identificar possíveis brechas de segurança ou regras desnecessárias.

Verificar a lógica por trás das regras para garantir a eficácia e relevância delas.

### 4.5.4 Logs e Monitoramento:

Verificar se os logs de firewall e antivírus estão sendo devidamente registrados e monitorados.

Analisar os registros para identificar padrões de tráfego suspeitos ou atividades maliciosas.

### 4.5.5 Atualizações e Patches:

Revisar a política de atualizações e patches para o firewall e antivírus.

Garantir que todos os dispositivos estejam atualizados com as últimas correções de segurança.

### 4.5.6 Desempenho e Eficácia:

Avaliar o desempenho do firewall e antivírus em termos de detecção de ameaças e tempo de resposta.

Verificar se as soluções implementadas estão protegendo a rede de maneira eficaz.

### 4.5.7 Conformidade e Regulamentações:

Verificar se as políticas de firewall e antivírus estão em conformidade com regulamentações pertinentes ao setor.

### 4.6. AUDITORIA – SUPERBOATCHAT

#### 4.6.1 Ferramentas Utilizadas

Analisar se o backup está ocorrendo, verificando se conversas antigas estão armazenadas.

#### 4.6.2 Análise das Conversas

Revise as conversas relevantes, de departamentos com alto risco de vazamento de dados pessoais.

Identificar informações ou comportamentos pertinentes à investigação ou à conformidade.

#### 4.6.3. Segurança e Privacidade

Assegure-se de que todas as informações sensíveis sejam tratadas com cuidado, seguindo políticas de segurança e privacidade.

Validar a senha e realizar a troca de tempos em tempos (Período sugerido 90 dias).

## 5. REGISTROS

Todos os registros das auditorias serão acessíveis por meio do sistema GLPI, proporcionando uma apresentação clara dos resultados e da efetividade dos controles vigentes.

## 6. REFERÊNCIA

LEI GERAL DE PROTEÇÃO DE DADOS- LGPD
IATF 16949 /ISO9001/ISO14001

## 7. DISTRIBUIÇÃO

Coordenadoria da qualidade
Tecnologia da Informação